Survivable Mobile Wireless Networks: Problems and Solution Directions for Dynamic Wireless Network Establishment, Key Management, and Vulnerability Assessment

Philip Campbell
Brian Van Leeuwen
William Young
Networked Systems Survivability and Assurance Department

Timothy Draelos
Mark Torgerson
Cryptography and Information Systems Surety Department

Sandia National Laboratories
P. O. Box 5800
Albuquerque, NM 87185-0785

October 31, 2001

ABSTRACT

This report is the result of short-term research at Sandia National Laboratories for Dr. Douglas Maughan at DARPA in three areas of survivable wireless networks: (1) dynamic wireless network establishment, (2) key management, and (3) wireless vulnerability assessment. As requested, we identified significant problems/objectives in each area and provide potential solution directions. This report assumes familiarity with wireless networks, their environments and purposes. An executive summary is provided immediately before the body of the report.

EXECUTIVE SUMMARY

This report is the result of short-term research at Sandia National Laboratories for Doug Maughan at DARPA in three areas of survivable wireless networks: (1) dynamic wireless network establishment, (2) key management, and (3) wireless vulnerability assessment. As requested, we identified significant problems/objectives in each area and provide potential solution directions.

1. Dynamic Wireless Network Establishment

Many future military communications systems will depend on mobile wireless networks that have dynamic topologies. These systems can vary in size, node density, communication range, data rate, and have a range of Information Assurance (IA) levels that require establishment and maintenance during the system life. The networks must function in the presence of adversarial, environmental, and operational stressors that may disrupt communications. Dynamic network establishment and maintenance is critical to the effective deployment of survivable mobile wireless networks in military environments.

Problem/Objective	Potential Solution Directions
Topology Validation Increase the security of wireless ad hoc network's topology control by mitigating the affects of adversarial manipulation of the control plane.	**Geographical data** A communicating node should validate that its network logical toplogy agrees with the network's geographical topology.
Network Management Provide an effective and secure method to disseminating network management data throughout a dynamic and decentralized network.	**Cluster-based architecture** Group network nodes in clusters to reduce the amount of update traffic required throughout the network. **Meta-data** Meta-data can effectively reduce the amount of network management control traffic necessary to maintain network operation.
Joining and Compromised Nodes Improve wireless and mobile ad hoc network survivability by controlling the scope of influence of new nodes and isolating compromised nodes.	**Proxy nodes** Network nodes have capability to control the types of data communicated to neighboring nodes based on established trust levels.
Control-Plane Survivability Improve wireless and mobile ad hoc network survivability by providing control plane redundancy.	**Hybrid protocols** Provide logical redundancy within the control protocol to ensure network operation when one control protocol may be impacted.

2. Survivable Key Management

The models of trust and vulnerabilities that guide standard key management solutions in the wired world do not necessarily map to the wireless world due to node mobility and operation in adversarial environments. To have the highest level of security, a network must have a Key Manager (KM) that oversees and takes responsibility for the key management process. However, the realities of a mobile, tactical environment make it difficult for a KM to accomplish its duties in all situations, requiring key management solutions that enable survivability.

Problem/Objective	Potential Solution Directions
Infrastructure Efficiency Provide a key management infrastructure that is efficient enough to allow its use in the mobile wireless environment.	**Hybrid cryptography** Combine the strengths of both symmetric and assymetric (public) key management techniques. **Efficient implementations** Efficient hardware cryptographic accelerators designed specifically for wireless devices.
Sub-Network Key Management Determine the key management duties that are appropriate for separated sub-networks to perform. Devise efficient techniques to accomplish these duties.	**Analysis of key management duties** Perform a fundamental analysis of the key management duties appropriate for a sub-network in the absence of the KM.
Trust Metrics Develop methods for nodes, including the KM, to measure trust in other nodes.	**Consensus protocols** Develop protocols that allow wireless nodes to reach consensus on important information. **Trust criteria and response policies** Develop criteria and metrics for trusting an entity and policies to act upon the metrics.

3. Vulnerability Assessment

Wireless networks employ different technologies than wired networks and are confronted with unique operational issues. Due to rapid innovations of this technology, meaningful vulnerability assessments of ad hoc wireless networks have not been performed. A vulnerability assessment identifies weaknesses within a particular device or system across a variety of areas - physical, logical, operational, architectural, etc. The proper application of assessment results will support vulnerability mitigation and design improvement, and enhance the survivability and evolving security-engineering efforts in wireless networks.

Problem/Objective	Potential Solution Directions
Wireless Vulnerability Assessment Develop necessary capabilities and perform vulnerability assessments of emerging wireless network architectures and technologies designed to support future tactical networks.	**Information assurance metrics** Develop clearly defined, measurable, replicable, and time-dependent metrics. **Methods and techniques** Develop assessment methods and techniques of OSI layers 2 and higher due to the variety of network routing protocols and the lack of integrated security within these protocols. **Tools** Develop tools that identify vulnerabilities in wireless protocols and test and verify the interfaces between wired and wireless networks.

The body of this report covers the three topic areas as follows: Section 2 addresses dynamic network establishment, Section 3 covers key management and Section 4 discusses wireless vulnerability assessments.

1. Introduction

Wireless communication networks are critical to many national security systems such as military systems. Military wireless networks often operate in adversarial environments, where an enemy may try to deny or corrupt network operations. In addition, the natural environment, such as weather, terrain, and foliage, also causes significant impacts to network operations. Information transmitted on these networks includes both network-control information and application-layer data. Although Information Assurance (IA) is recognized as a critical aspect in protecting and disseminating user and control data, current IA approaches in the wired environment often do not directly apply to wireless networks. Current wireless IA approaches focus primarily on physical layer solutions, and do not consider the unique aspects of other communication layers within the wireless system.

Sandia participated in a DARPA effort focused on identifying the hurdles preventing the realization of survivable mobile wireless communication networks. This effort supports DARPA's continuing and developing interests in mobile wireless networks for military systems. Under DARPA's direction, Sandia investigated issues in the following two topical areas:

- Dynamic wireless network establishment
- Survivable key management and infrastructure capabilities

The content of this report includes identification of problems and potential solution directions relating to the above topics. Given our experience in network assessments and our belief that the topic warranted additional attention, we also identified some wireless vulnerability assessment issues. Thus, we include a discussion on:

- Vulnerability assessments of wireless networks

The body of this report covers the three topic areas as follows: Section 2 addresses dynamic network establishment, Section 3 covers key management and Section 4 discusses wireless vulnerability assessments.

2. Dynamic Wireless Network Establishment

Many future military communications systems will depend on mobile wireless networks that have dynamic topologies. These systems can vary in size, node density, communication range, data rate, and have a range of Information Assurance (IA) levels that require establishment and maintenance during the system life. The networks must function in the presence of adversarial, environmental, and operational stressors that may disrupt communications. Dynamic network establishment and maintenance is critical to the effective deployment of survivable mobile wireless networks in military environments.

Sections 2.1 through 2.4 describe specific problems that must be addressed to ensure effective deployment of systems that depend on wireless networks.

2.1. Location Dependent Topology Validation

2.1.1. Problem/Objective - *Increase the security of wireless ad hoc network's topology control by mitigating the affects of adversarial manipulation of the control plane.*

A critical attribute of a wireless ad hoc network is its availability to communicate information required by network nodes. Networks attempt to maintain availability in the presence of denial of service (DOS) attacks. A critical element of maintaining availability in a wireless ad hoc network is the ability to securely transmit network control-plane data throughout the network. An adversary may disrupt network operation by interfering with control-plane data that must be communicated throughout the ad hoc network.

Cryptographic approaches, such as digital signatures, have been proposed to secure the control-plane data. Not only do digital signatures come with a significant overhead cost, they typically follow a bolt-on approach, and in general, enhance security only marginally. Under certain adversarial models these control-plane data messages cannot be secured even with cryptographic authentication [5].

If an adversary has access to the communications channel he can record and rebroadcast control messages. The adversary may then have the ability to initiate selective jamming or choose to disrupt the communication by recording and replaying messages, which may cause the network to become partitioned. Suppose the adversary sets up a series of repeaters distributed throughout the physical mobile network as shown in Figure 1. The repeaters hear network traffic, and then transmit the traffic (possibly out of band) to all other repeaters. Then network traffic is broadcast back in band at the new location.

Since the adversary's repeaters have only increased the broadcast range of the mobile nodes and have not violated any of the security features, the topology control protocol may behave as though nothing happened. Each node will believe there is a much different network topology than actually exists. The adversary's repeaters give the nodes the false belief that the diameter of the network is much smaller than it actually is. The adversary is then free to selectively filter any application-layer data or control-plane data passing through its repeaters, or the adversary may simply eliminate the channel thus partitioning the network.

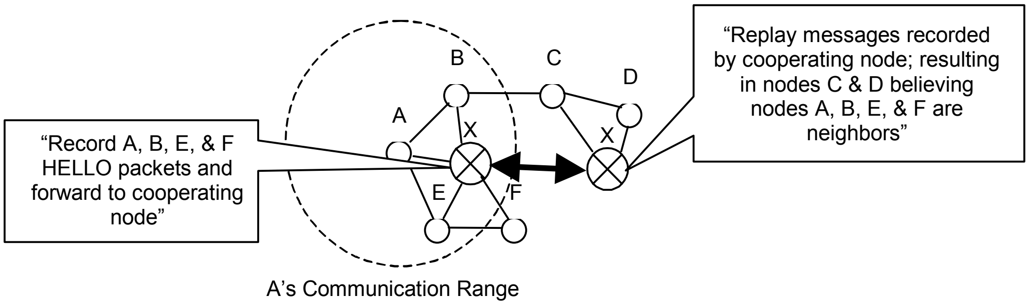
"Record A, B, E, & F HELLO packets and forward to cooperating node"
A
B
C
D
E
F
X
X
"Replay messages recorded by cooperating node; resulting in nodes C & D believing nodes A, B, E, & F are neighbors"
A's Communication Range

Figure 1. Two adversary nodes cooperating by recording and replaying control messages.

2.1.2. Solution Directions

A solution is for network nodes only to communicate with radios from its fellow network nodes. Since any digital authentication can be replicated in the replay attack the radios will have to depend on some form of waveform authentication to verify the authenticity of a node. However, this may become quite complex as the ad hoc network increases in size and each node's radio waveform must be characterized. In addition, approaches to TRANSEC may provide sophisticated spread spectrum waveforms that are not easily recorded and repeated.

If a node were aware of the other node's location it could validate that its logical topology agreed with its geographical topology. For example if a node's radio has an ability to communicate 300 meters and its geographical distance is greater than 300 meters than the node should suspect the data. This idea can also be extended to other forms of logical inconsistencies in data that is shared amongst nodes.

A node can obtain geographical data from GPS and include its location in its communications. This will allow nodes to verify that their radio communication distance and direction agree with actual node geographical separation. In some applications GPS may not be available or may be easily jammed by an adversary. In these situations methods that depend on some form of inertial navigation can be used in conjunction with GPS.

2.2. Wireless and Mobile Ad Hoc Network Management

2.2.1. Problem/Objective - *Provide an effective and secure method to disseminating network management data throughout a dynamic and decentralized network.*

Many network-centric systems depend on wireless communication to maintain connectivity between mobile nodes. Network-centric systems can be comprised of a large number of nodes with varying capabilities and resources among the nodes. The systems will be deployed in situations that change very quickly and the network must be dynamic to change with its operation environment. Node movement that leads to network topology changes are addressed with dynamic self-configuring routing protocols that exchange routing-control data to direct application-layer data. A number of research efforts are developing effective protocols to establish and maintain network routing capabilities.

However, an effective network-centric system requires more than simply communicating routing control data throughout the network. These networks also require network *management data* to be communicated throughout the network. An overall network management scheme is necessary to effectively address the following network issues:

- Configuration management
- Fault management
- Security and survivability management
- Performance management
- Accounting management

Methods for exchanging the above listed control-data must be available throughout the lifetime of the network. The control-data from the various areas impact the network's dynamic protocol selection or parameter selection of the controlling protocols. For example, performance and accounting measurements will impact the routing protocol selection or the security system selection in a highly dynamic network. As network nodes experience fault occurrences the network must be able to respond to maintain its effectiveness. Configuration management includes network initialization of potentially a large number of nodes that cannot be done manually. Some networks may have both offensive and defensive roles that may require different security requirements and an ability to quickly change the security systems to meet the changing role of the network-centric system. An example is a network that can use more of its resources for security during defensive monitoring and switch to less resource demanding security during offensive attacks that may require shifting resources to more critical needs. These scenarios require network management capabilities.

Also managing the different types of data the network may be transmitting such as voice, video, sensor data, or command data may require network configuration changes. The data types may have different link requirements related to bandwidth, latency, security, and/or reliability. These varying network operation scenarios require methods to control and reconfigure the network.

A recent paper [1] has presented a protocol that addresses a number of these issues. However, their approach is based on a single clustering algorithm and it is necessary to research management architectures and protocols that apply to other grouping methods.

2.2.2. Solution Directions

The purpose of network management is to provide a control mechanism that optimizes the effectiveness of the network in its operational environment. Potential solutions must consider that a wireless ad hoc network operates in a resource-constrained environment. The management approach must not create a large amount of overhead traffic that consumes network bandwidth capacity and node resources. The approach should be secure so as to not create additional network vulnerabilities. Initial direction should investigate the best network architecture (how nodes are grouped) to implement a secure management approach. The overall network management approach will consist of two parts:

- A management architecture that specifies what aspects of the network will be managed
- A network management protocol that specifies how the management is performed and includes the description of control messages

A network management solution can be considered as a layer that participates above the routing control layer. Network management will use the services of a routing layer and will depend on this layer to provide control message delivery. Node applications may use services from the network management layer or interact with the routing control directly. Each of the services has security applied to all messages as shown in Figure 2.

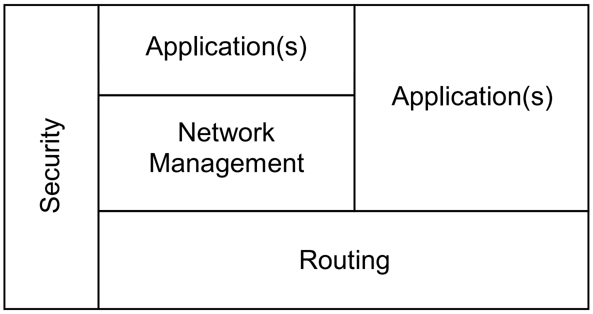

Figure 2. Network management protocol location in node protocol stack.

Possible solution directions include approaches for grouping network nodes such as clustering to effectively reduce the amount of update traffic required throughout the network. A spanning tree approach could be used to improve the efficiency of network overhead data collection.

A solution will likely be based on a decentralized approach to avoid creating a single point of failure in the system. Consideration should be given to using meta-data to support the network management approach. Meta-data will allow nodes to provide small data packets indicating that specific information is available from the node. If a receiving node requires the information and can authenticate itself, then the larger complete data set is sent.

Effective and secure multicasting approaches will be needed to distribute network management information throughout the network.

Policy-based management approaches may also be a component in managing the ad hoc network. The goal is to control the role and behavior of network elements and resources by defined rules. These policies could be brokered by a distributed set of ad hoc network policy servers.

2.3. Restriction of Data Flows for Joining and Compromised Nodes

2.3.1. Problem/Objective - *Improve wireless and mobile ad hoc network survivability by controlling the scope of influence of new nodes and isolating compromised nodes.*

The entry and reentry of nodes in wireless ad hoc networks requires an authentication process to ensure the integrity of the nodes requesting connectivity to the network. In an ad hoc network, the concept of a base station does not exist, and nodes connect on a peer-to-peer basis. The authentication process, whether based on a central authentication authority or a distributed threshold approach, may take a significant amount of time. Routing tables, topology updates, key updates, and other network control information should not be forwarded to an unauthenticated node. This impacts the convergence time of the network, as well as the overall connectivity of the network at any given time.

The ability to forward a limited amount of data while also restricting the influence of a node requesting entry into the network offers significant benefits to tactical network operations and security. A wireless network should support the isolation of compromised nodes without disrupting the operations of the network as a whole, even after those nodes complete an authentication process. In addition, restriction of data flow based on levels of trust requires some filtering abilities by individual nodes. A minimum reliance on cryptographic processes represents a primary design goal so as to minimize the processing overhead required to maintain the integrity of the filtering process.

2.3.2. Solution Directions

A solution direction is to provide network nodes with a capability to limit the types of data communicated to neighboring nodes. This approach can be summarized as:

- Allow ad hoc nodes to serve as proxies for other nodes that wish to join the network
- Apply a dynamic firewall on connection to joining or compromised nodes
- Filter data at OSI Layers 2 and 3 to restrict control and application-layer data flows
- Use network management to augment configuration control of the filtering

The suggested approaches and combinations thereof would support either threshold or central authority-based node authentication mechanisms. The firewall configuration would be updated as the trust level associated with the new node increases. A recently entering node could be provided a subset of information upon initial authentication by the directly connected proxy node, with a range of influence increased as the authentication is provided by other sources, i.e., other nodes or a central authority.

Some wired infrastructure efforts that consider aspects related to the proposed security approach are found in [6, 7, 8].

2.4. Control Plane Survivability

2.4.1. Problem/Objective - *Improve wireless and mobile ad hoc network survivability by providing control plane redundancy.*

Wireless and mobile ad hoc networks require connection redundancy, path discovery, or network re-convergence, in order to handle link and/or node failures. In the tactical environment, rapid movements, harsh physical environments, and adversaries all contribute to these failures. Multiple paths to destinations provided survivability within the network, but may be difficult to maintain. In addition, the security constructs necessary to create a secure wireless network must be updated as the topology and participants in the network change. Control-plane data is critical to maintaining network connectivity and security, and must be effectively disseminated to ensure the secure communication of application-layer data.

Required response times for future tactical networks will likely be faster than the routing protocols can support in a typical topology recovery operation. As these wireless nodes will supply connection to robotic platforms, as well as connection to command and control centers for both human and robotic elements, a significant portion of the application-layer traffic will not be local to a given subset of nodes. In addition, as wireless nodes increase in sophistication, including the use of directional antennas and concurrent use of multiple frequencies (different from frequency hopping), the control data associated with an individual node is likely to increase. The effective integration of all these elements requires robust control data dissemination methods. A single routing algorithm does not resolve all these issues, and even a hybrid routing approach, such as the Zone Routing Protocol (ZRP) [4], faces limitations. ZRP utilizes both reactive and proactive protocols, but the proactive protocol is limited to the local region, typically less than 6 hops, while the reactive protocol provides distant connectivity. This approach places the emphasis on rapid local connectivity, which may not be the requirement of the application.

2.4.2. Solution Directions

Solution directions include the following:

- Utilize protocols with significantly different characteristics to disseminate control data.
- Develop hybrid control data that supports multiple routing protocols
- Identify minimum subsets of control data required to maintain responsiveness of the network

The use of two different protocols for disseminating control data, with significantly different characteristics, i.e. proactive versus reactive, may provide a method of logical redundancy within a tactical ad hoc network. Control data could make use of different routes to distribute subsets of control data, in order to maintain the responsiveness of the network. These types of solution will likely require the development of hybrid control data that supports multiple routing protocols.

A current effort that addresses some of the problems outlined in the previous section is presented in [9]. The operation of security protocols is not directly considered in the effort. Routing protocol and behavior must ensure the security protocols are aptly supported.

3. Survivable Key Management

The models of trust and vulnerabilities that guide standard key management solutions in the wired world do not necessarily map to the wireless world due to node mobility and operation in adversarial environments. Caution is therefore advised when considering the use of cryptography in wireless networks and advances to key management survivability are necessary. This section presents three problems that must be addressed to enable a key management system to operate and survive in an adversarial wireless environment.

To have the highest level of security, a network must have some entity that oversees and takes responsibility for the key management process. We will call this well-protected authority the Key Manager (KM). The hierarchical nature of the military command structure makes an easy fit for the proper operation of a KM. The operational procedures associated with key management can be enforced as a matter of course. Nodes can be initialized properly. Keys can be generated, distributed, and installed according to the highest standards of security. However, the realities of a mobile, tactical environment make it difficult for a KM to accomplish the rest of its duties in all situations.

Three hard problems standing in the way of realizing survivable key management in wireless networks are 1) providing an efficient key management infrastructure, 2) determining and satisfying the key management duties in sub-networks that have no contact with the KM, and 3) developing methods for measuring trust in network nodes.

3.1. Necessity of an Efficient Key Management Infrastructure

3.1.1. Problem/Objective - *Provide a key management infrastructure that is efficient enough to allow its use in the mobile wireless environment.*

In practice, the resource constraints imposed by the mobile wireless environment make it difficult or impossible to actually accomplish all of the key management duties in a variety of scenarios. Current public key techniques are wonderfully suited to bring all of the security services that a network would desire except that they are, in general, impractical in a tactical mobile wireless environment due to resource limitations. On the other hand, symmetric key techniques are orders of magnitude more efficient, however, a purely symmetric key infrastructure is much more difficult to manage than a Public Key Infrastructure (PKI).

3.1.2. Solution Directions

The cryptographic community has put a great deal of effort into the optimization of existing cryptographic techniques. The community is also actively engaged in devising more efficient protocols. However, there are a couple of areas that have not received tremendous scrutiny and may pay great efficiency dividends. Both of the following solution directions need to incorporate survivable attributes in their design and implementation.

- ➢ Hybrid cryptography – blending of symmetric and asymmetric cryptographic techniques. The hybrid approach may take strengths and weaknesses from each method in order to create a cryptographic infrastructure that is both manageable and efficient.

- Efficient hardware cryptographic accelerators designed especially for wireless devices. Designs for both Application Specific Integrated Circuits (ASIC) as well as for Field Programmable Gate Arrays (FPGA).

3.2. Sub-network Key Management

3.2.1. Problem/Objective - *Determine the key management duties that are appropriate for separated sub-networks to perform. Devise efficient techniques to accomplish these duties.*

In a mobile environment, it is inevitable that a certain portion of the network will lose contact with the KM. For the network to have any notion of survivability, the sub-network that has separated from the KM would still need to function securely, but it is not possible to consistently execute the same level of key management in a portion of the network that has separated from the KM. It seems as though the best a node can do in a network partition is to rely on its peers to emulate the authority or else the node must perform its own key management services. There has been little research into the impacts and consequences of a radical change in the key management structure.

3.2.2. Solution Directions

A solution direction is the following:

- A fundamental analysis of the key management duties that are appropriate for a sub-network to conduct in the absence of the KM must be accomplished.

Threshold cryptography can be used by a group of resourceful nodes to provide a robust method of performing certain key management services. For instance threshold cryptography may provide a method to reduce the impacts of single points of failure. However, the use of threshold cryptography can by no means be a complete substitute for the security features provided by the KM.

- The logic behind sub-network use of threshold cryptography must be examined. In many cases there may be no security benefit added with the use of threshold cryptography. A careful survey of the key management services and the security benefits provided (and not provided) by threshold cryptography must be conducted.
- The computational, and bandwidth requirements associated with threshold cryptography are extreme and are generally more than a mobile network can support. Better methods tailored to interim key management of wireless devices need to be devised.

3.3. Trust Metrics

3.3.1. Problem/Objective - *Develop methods for nodes, including the KM, to measure trust in other nodes.*

The adversarial nature of military tactical environments and the portability of mobile devices demand that a KM have a way of detecting and expelling compromised nodes as well as having the ability to recover from a compromise. Even when a KM is available for key management services, a single compromised node can wreak significant havoc on a military mission. Certainly for public key systems there are reasonably robust methods for a KM to expel compromised nodes. However, it is not clear that damage control can be addressed by cryptographic means. For example, when an adversary corrupts a database or reads private messages, what one does in response to such actions appears to be non-cryptographic in nature. Finally, recovering from adversarial manipulation naturally follows the detection of the manipulation and removal of the node.

As mentioned above, each node in a partitioned sub-network must assume some of its own key management responsibilities. Nodes must be able to measure the likelihood of a compromise and decide when or if to discontinue communication with a particular node. In order for any meaningful decisions to be made, each node must have a set of metrics to measure the level of trust in the other nodes. In some cases, nodes may have human operators whose trust must also be measured. The metrics might be a function of the time that each communicating node was out of contact with the KM, the length of time since credential expiration, the environment, the sensitivity of the information being conveyed, information from peer nodes, confidence in key protection, as well as other factors.

When a sub-network is reinstated into the main network, the KM must be able to judge how much effort is needed to restore proper security to the network. If a node has been out of contact for an extremely long time, then the only recourse may be to recall the node so that it may be physically inspected and reinitialized. The KM as well as the other nodes in the network must have criterion to decide if such an effort is needed.

3.3.2. Solution Directions

At best, measuring trust is difficult. However, even in a highly dynamic environment there are rules, procedures, and policies that can be followed. It is this basic set of operational criterion that must be developed.

- Develop consensus protocols for wireless networks.
- Develop assessment/evaluation criteria for trusting an entity.
- Develop trust metrics that apply to an operational environment.
- Develop policies and procedures to act upon the metrics.

4. Wireless Vulnerability Assessment

Wireless networks employ different technologies than wired networks and are confronted with unique operational issues at each layer of the communications stack. Due to rapid innovations of this technology, meaningful vulnerability assessments of ad hoc wireless networks have not been performed. A vulnerability assessment identifies weaknesses within a particular device or system across a variety of areas - physical, logical, operational, architectural, etc. The proper application of assessment results will support vulnerability mitigation and design improvement, and enhance the survivability and evolving security-engineering efforts in wireless networks. Without an assessment and understanding of the vulnerabilities of a system, it becomes impossible to perform risk management for that system.

4.1. Metrics, Methods, Techniques, and Tools for Wireless Network Vulnerability Assessments

The area of wireless networking is relatively new and the area of vulnerability assessment is only slightly more mature. However, the emphasis of this section is to identify work needed to extend current vulnerability assessment into the wireless network world.

4.1.1. Problem/Objective – *Develop necessary capabilities and perform vulnerability assessments of emerging wireless network architectures and technologies designed to support future tactical networks.*

The flexibility and benefit that wireless networks offer tactical operations, including combat initiatives, humanitarian efforts, and logistics, also introduces new vulnerabilities to the communication system. Wireless protocols, network architectures, node identification, network addressing, key distribution, etc. represent some of the areas where vulnerabilities unique to wireless networks start to surface. For example, [3, 5] discusses some of the vulnerabilities in emerging ad hoc routing protocols. An understanding of unique wireless vulnerabilities supports design improvement of the previously mentioned areas, particularly in the context of survivability and security. An understanding of vulnerabilities that can be opened in a system as a side effect of adding wireless networks to that system are also of concern. However, sufficient detail on all such vulnerabilities currently does not exist.

Successful vulnerability assessments require metrics, methods, techniques, and tools. In the wired networking environment, many of these assessment components are still immature, and in the wireless environment, the deficiency is even more severe. Vulnerability assessments of the physical layer and the RF transmission medium receive significant attention in the wireless environment, but the networking and transport layers, as well as optical transmission media issues, are currently not well addressed.

4.1.2. Solution Directions

Vulnerability assessments require work in three categories to be of sufficient use. Those three principal categories requiring research and development to extend vulnerability assessment into the wireless networking area are as follows:

- ➢ *IA metrics* must be clearly defined, measurable, replicable, and time-dependent. IA metrics measure the effectiveness of security only against what is known, and new vulnerabilities and attacks will likely not be covered [2]. For this reason, IA metrics must evolve as new vulnerabilities are discovered, and hence, metric development and refinement is a critical component of vulnerability assessments.

  Specific metrics for wireless networking have not been defined. Metrics currently used for assessing wired networks must be investigated to determine their use in a wireless environment.

- ➢ *Methods and techniques* that focus on OSI layers 2 and higher must be developed due to the variety of network routing protocols and the lack of integrated security within those protocols. Identification of assumptions made in the development of layer 2 and greater protocols that allow vulnerabilities in wireless networks is a concern. Also, most of the methods and techniques available for wireless networks focus on the RF transmission media, but research into optical networks demands new vulnerability tools for wireless optical assessments.

- ➢ *Tools* specific to secure wireless networking also lack the sophistication necessary for accurate security engineering and evaluation. For example, the inclusion of security protocols in wireless simulation packages such as OPNET will identify weaknesses in those protocols. Vulnerabilities created by scalability limitations can be identified through improved simulation capabilities. Tools that are currently used to examine the vulnerabilities in wired networks will need to be extended to provide a similar service to wireless networks. Tools will also need to be developed that test and verify the interfaces between wired and wireless networks.

5. References

[1] W. Chen, N. Jain, and S. Singh, *ANMP: Ad Hoc Network Management Protocol,* IEEE Journal on Selected Areas in Communications, August, 1999.

[2] N. Bartol, N. Givans, *IA Metrics: Critical Review & Technology Assessment Report,* Information Assurance Technology Analysis Center, Falls Church, VA 22042, June 1, 2000.

[3] J. Lundberg, *Routing Security in Ad Hoc Networks*, Tik-110.501 Seminar on Network Security, Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2000.

[4] C. Perkins, *Ad Hoc Networking*, Addison-Wesley, 2001.

[5] M. Torgerson and B. Van Leeuwen, *Routing Data Authentication in Wireless Ad Hoc Networks,* Sandia National Laboratories, SAND Report 2001-3119, October 2001.

[6] http://www.darpa.mil/ito/psum2000/J905-1.html

[7] http://www.darpa.mil/ito/psum2000/J043-0.html\

[8] http://www.eecis.udel.edu/~yzhu/17sac08-wchen.pdf

[9] http://www.ir.bbn.com/projects/dawn/dawn-index.html